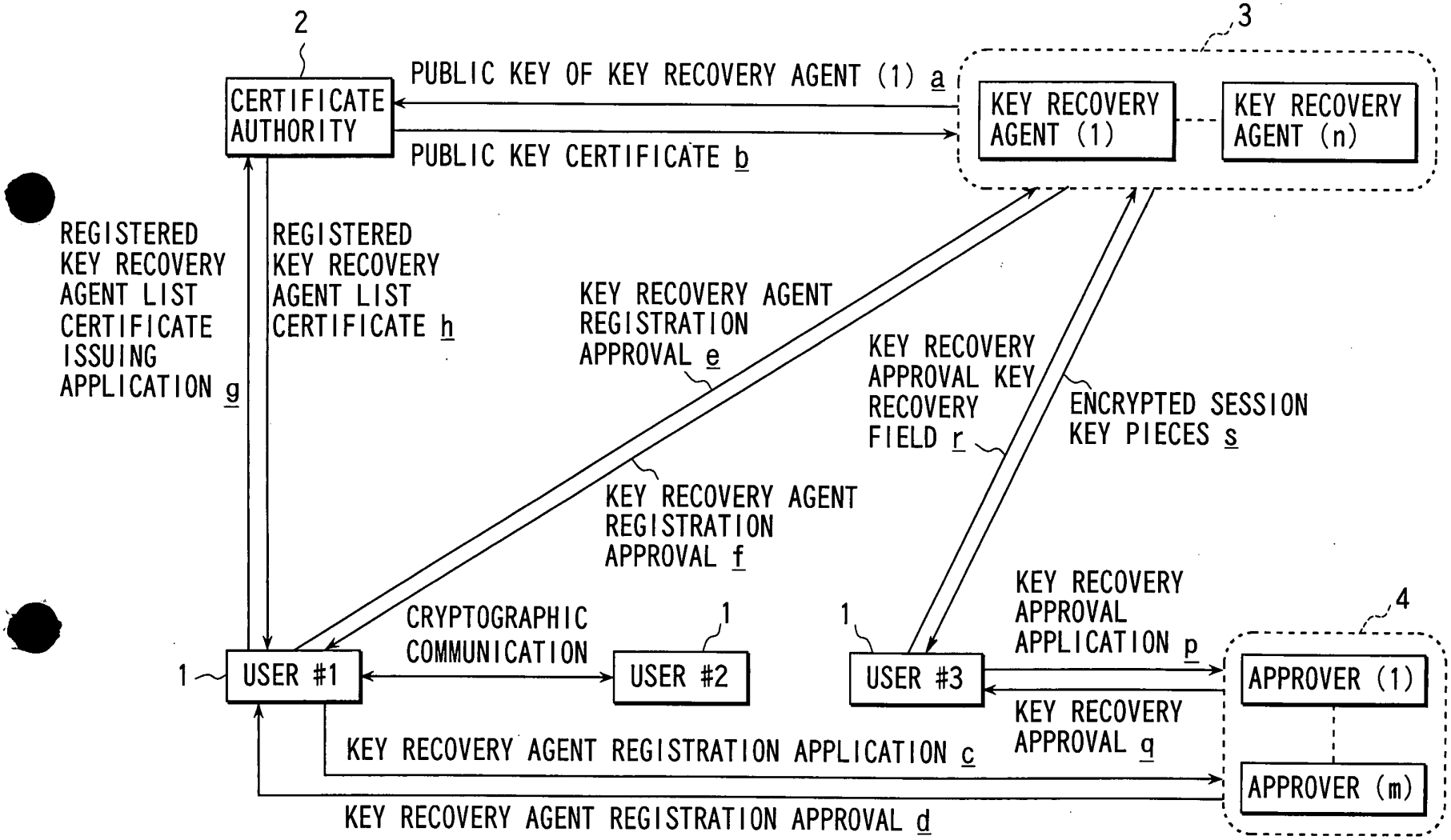
2
3
CERTIFICATE AUTHORITY
PUBLIC KEY OF KEY RECOVERY AGENT (1) a
PUBLIC KEY CERTIFICATE b
KEY RECOVERY AGENT (1)
KEY RECOVERY AGENT (n)
REGISTERED KEY RECOVERY AGENT LIST CERTIFICATE ISSUING APPLICATION g
REGISTERED KEY RECOVERY AGENT LIST CERTIFICATE h
KEY RECOVERY AGENT REGISTRATION APPROVAL e
KEY RECOVERY APPROVAL KEY RECOVERY FIELD r
ENCRYPTED SESSION KEY PIECES s
KEY RECOVERY AGENT REGISTRATION APPROVAL f
KEY RECOVERY APPROVAL APPLICATION p
CRYPTOGRAPHIC COMMUNICATION
1
1
1
4
USER #1
USER #2
USER #3
APPROVER (1)
KEY RECOVERY APPROVAL q
KEY RECOVERY AGENT REGISTRATION APPLICATION c
APPROVER (m)
KEY RECOVERY AGENT REGISTRATION APPROVAL d

FIG.1

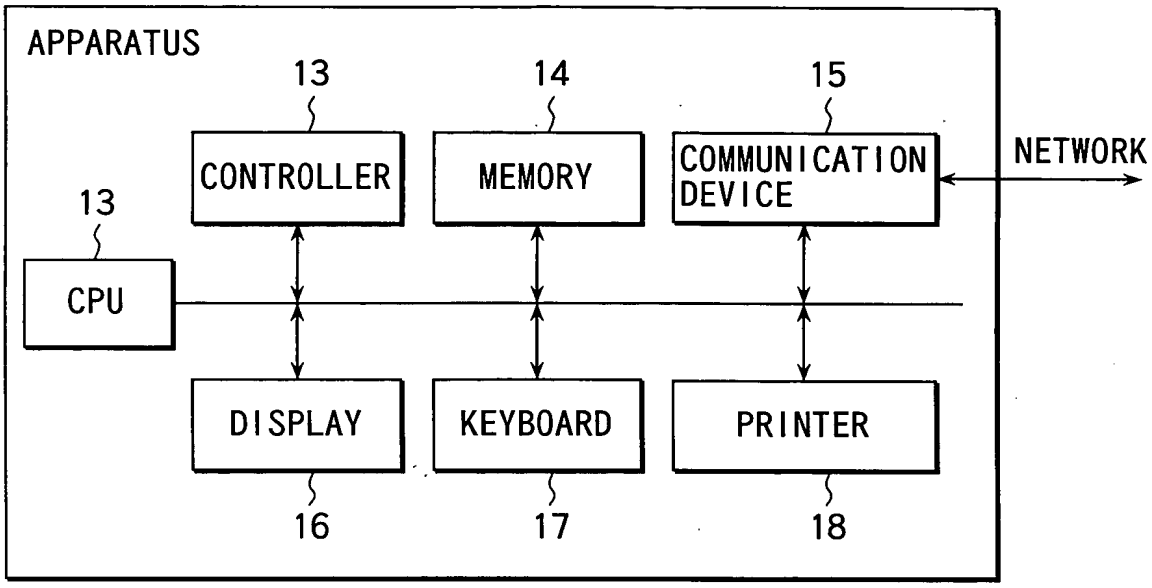
APPARATUS
13
14
15
CONTROLLER
MEMORY
COMMUNICATION DEVICE
NETWORK
13
CPU
DISPLAY
KEYBOARD
PRINTER
16
17
18

FIG.2

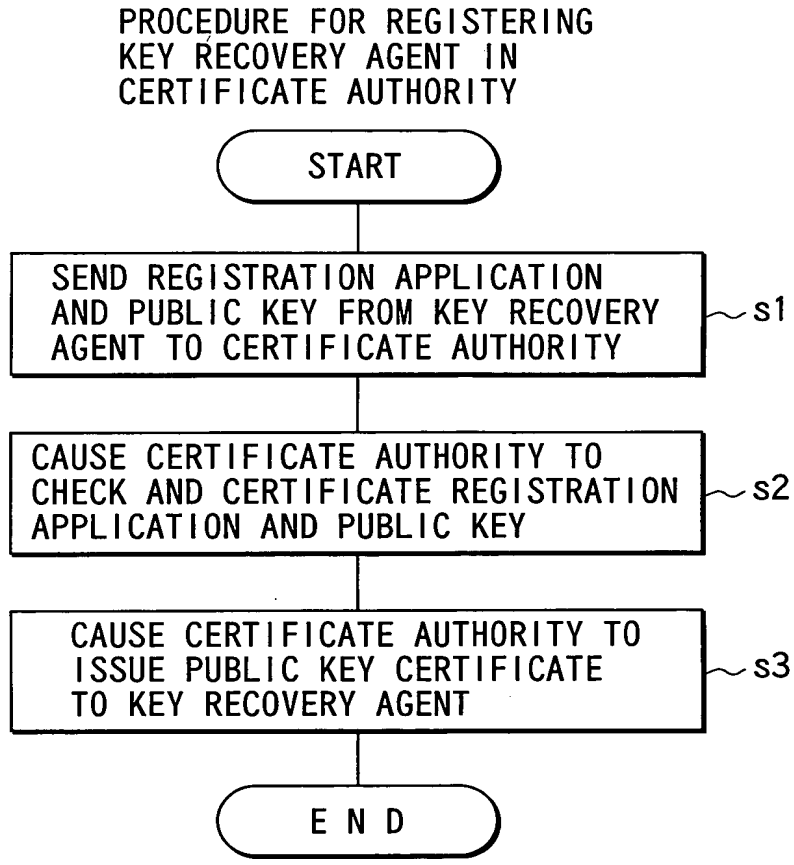
PROCEDURE FOR REGISTERING KEY RECOVERY AGENT IN CERTIFICATE AUTHORITY
START
SEND REGISTRATION APPLICATION AND PUBLIC KEY FROM KEY RECOVERY AGENT TO CERTIFICATE AUTHORITY
s1
CAUSE CERTIFICATE AUTHORITY TO CHECK AND CERTIFICATE REGISTRATION APPLICATION AND PUBLIC KEY
s2
CAUSE CERTIFICATE AUTHORITY TO ISSUE PUBLIC KEY CERTIFICATE TO KEY RECOVERY AGENT
s3
E N D

FIG.3

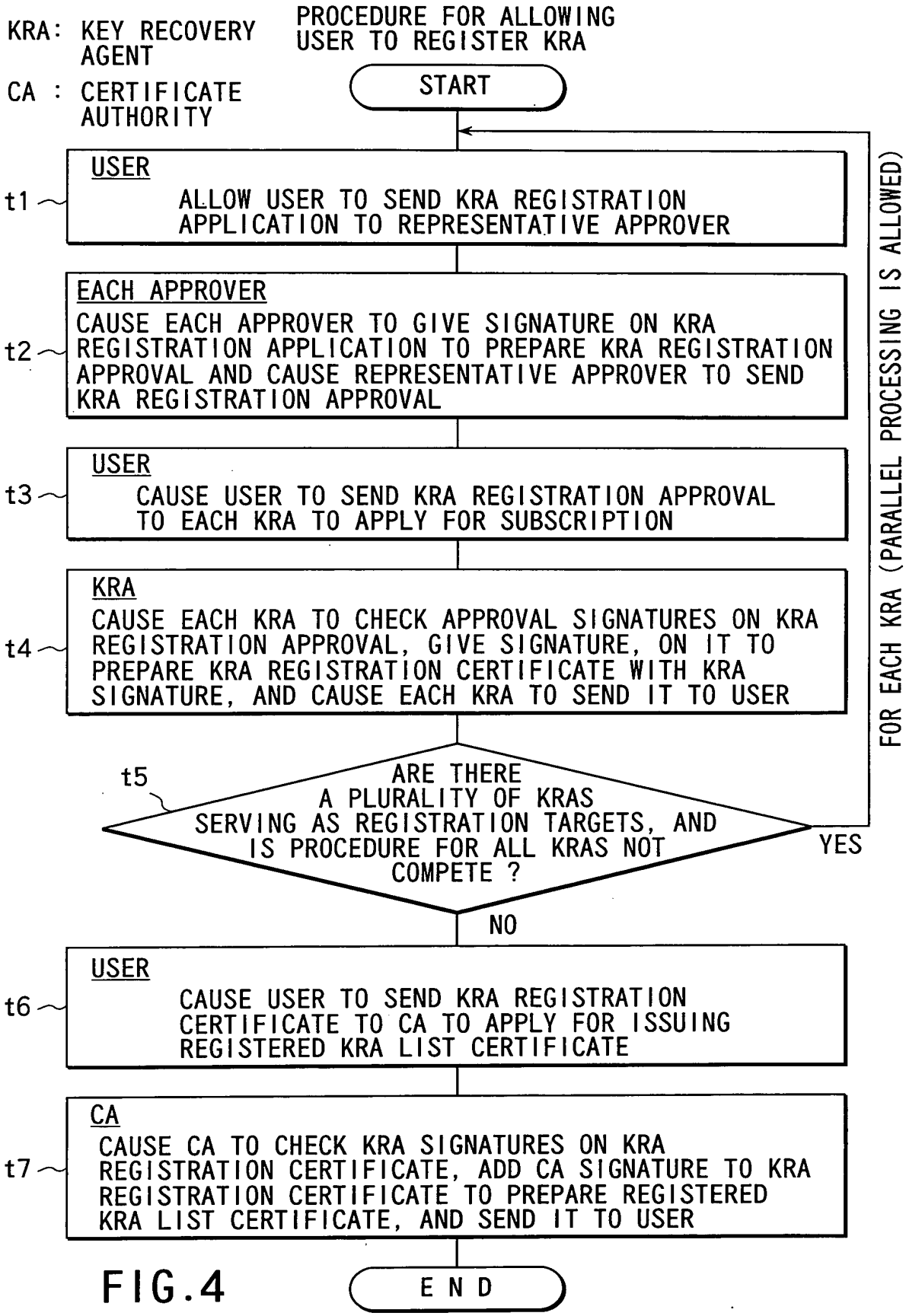
KRA: KEY RECOVERY AGENT
CA : CERTIFICATE AUTHORITY
PROCEDURE FOR ALLOWING USER TO REGISTER KRA
START
t1
USER
ALLOW USER TO SEND KRA REGISTRATION APPLICATION TO REPRESENTATIVE APPROVER
t2
EACH APPROVER
CAUSE EACH APPROVER TO GIVE SIGNATURE ON KRA REGISTRATION APPLICATION TO PREPARE KRA REGISTRATION APPROVAL AND CAUSE REPRESENTATIVE APPROVER TO SEND KRA REGISTRATION APPROVAL
t3
USER
CAUSE USER TO SEND KRA REGISTRATION APPROVAL TO EACH KRA TO APPLY FOR SUBSCRIPTION
t4
KRA
CAUSE EACH KRA TO CHECK APPROVAL SIGNATURES ON KRA REGISTRATION APPROVAL, GIVE SIGNATURE, ON IT TO PREPARE KRA REGISTRATION CERTIFICATE WITH KRA SIGNATURE, AND CAUSE EACH KRA TO SEND IT TO USER
t5
ARE THERE A PLURALITY OF KRAS SERVING AS REGISTRATION TARGETS, AND IS PROCEDURE FOR ALL KRAS NOT COMPETE ?
YES
FOR EACH KRA (PARALLEL PROCESSING IS ALLOWED)
NO
t6
USER
CAUSE USER TO SEND KRA REGISTRATION CERTIFICATE TO CA TO APPLY FOR ISSUING REGISTERED KRA LIST CERTIFICATE
t7
CA
CAUSE CA TO CHECK KRA SIGNATURES ON KRA REGISTRATION CERTIFICATE, ADD CA SIGNATURE TO KRA REGISTRATION CERTIFICATE TO PREPARE REGISTERED KRA LIST CERTIFICATE, AND SEND IT TO USER
END

FIG.4

REGISTERED INFORMATION TABLE 21

ID OF USER, APPROVER, AND KEY RECOVERY AGENT (22)	PUBLIC KEY WITH SIGNATURE OF CERTIFICATE AUTHORITY (23)	AGENT LIST REGISTERED BY USER (24)
USER #1	○○○○	A,B,C,
USER #2	××××	B,D,G,H
APPROVER α	△△△△	NONE
APPROVER β	□□□□	NONE
AGENT A	＊＊＊＊	NONE
AGENT B	▽▽▽▽	NONE

FIG.5

RECEPTION/TRANSMISSION OF CIPHER MESSAGE

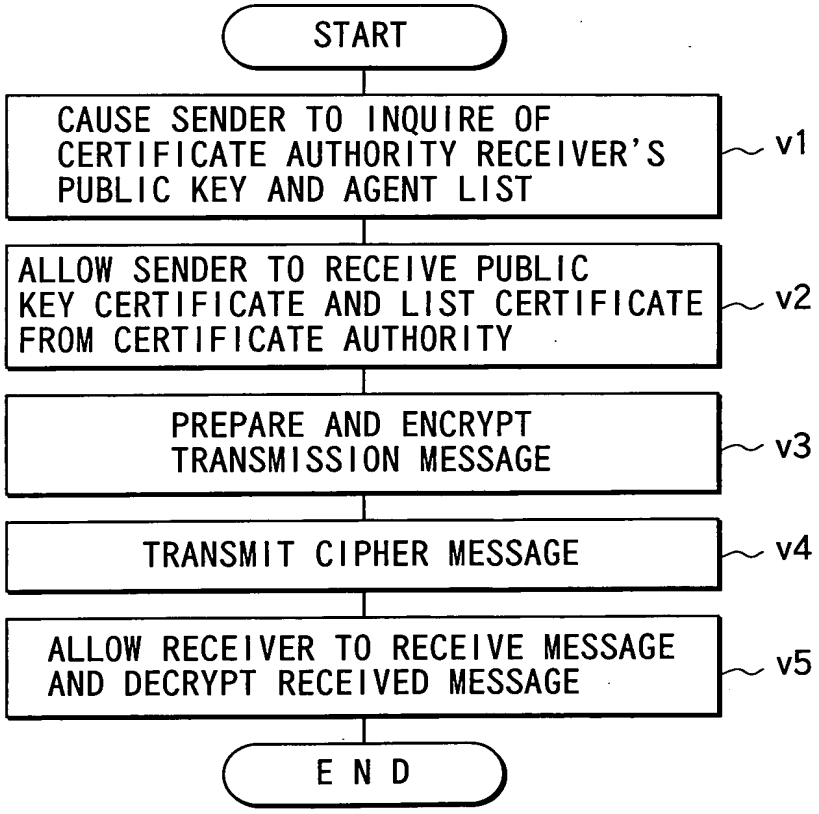

FIG.6

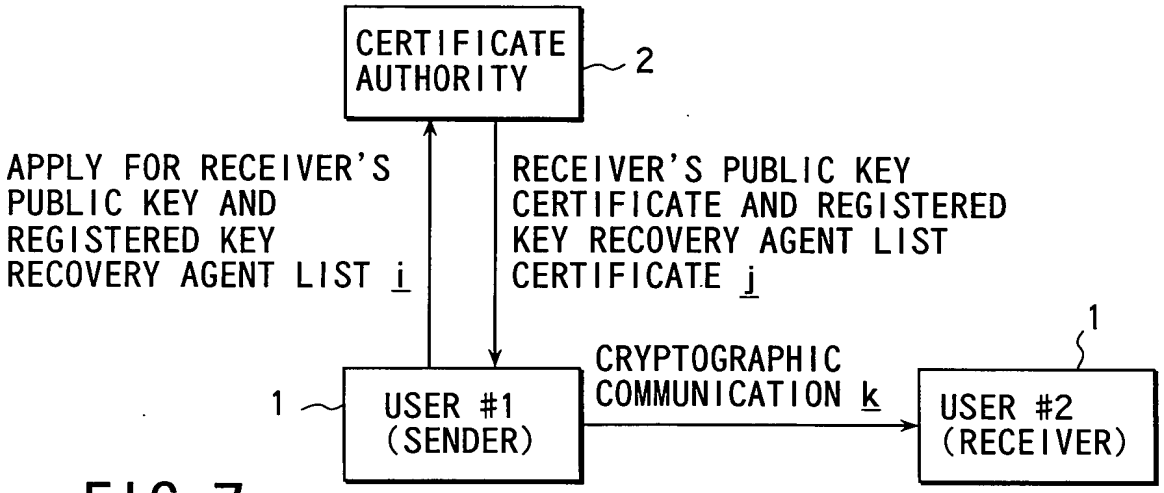

FIG.7

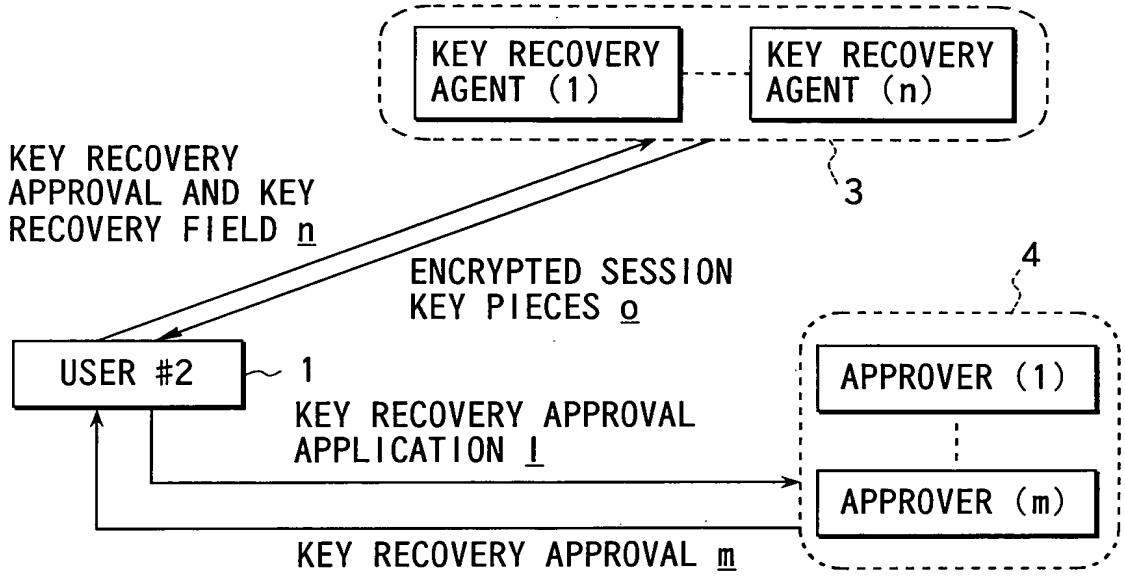

FIG.10

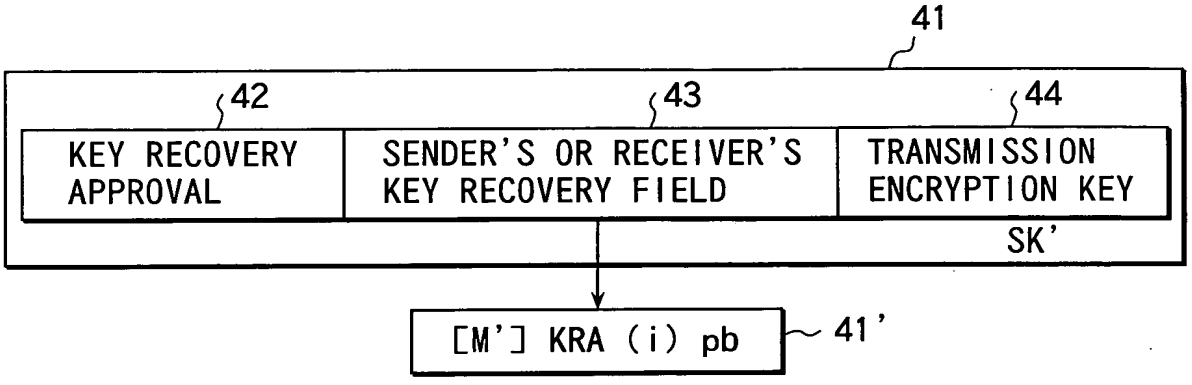

FIG.11

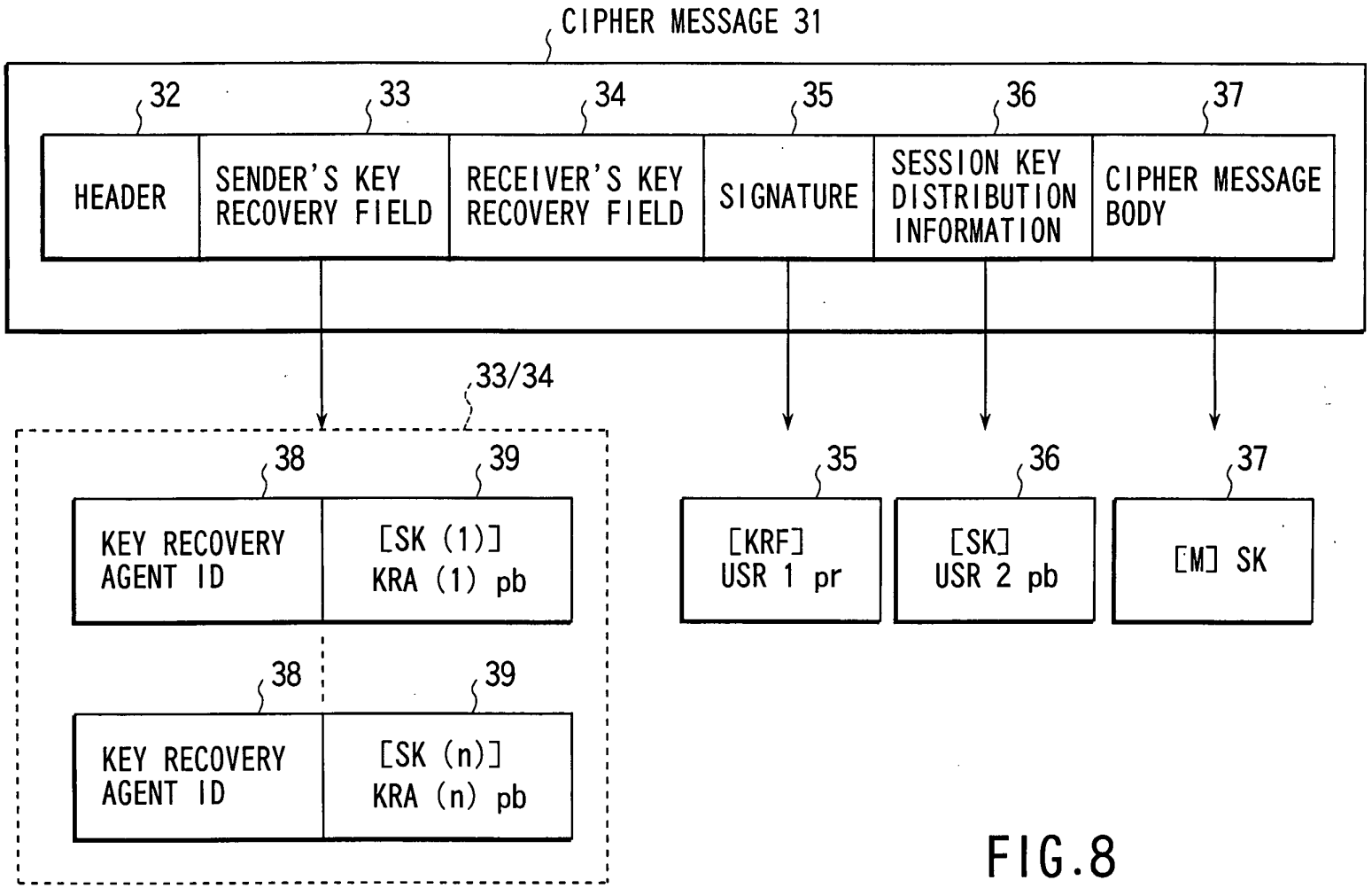
CIPHER MESSAGE 31
32
33
34
35
36
37
HEADER
SENDER'S KEY RECOVERY FIELD
RECEIVER'S KEY RECOVERY FIELD
SIGNATURE
SESSION KEY DISTRIBUTION INFORMATION
CIPHER MESSAGE BODY
33/34
38
39
KEY RECOVERY AGENT ID
[SK (1)] KRA (1) pb
38
39
KEY RECOVERY AGENT ID
[SK (n)] KRA (n) pb
35
36
37
[KRF] USR 1 pr
[SK] USR 2 pb
[M] SK

FIG.8

PROCEDURE FOR KEY RECOVERY BY SENDER OR RECEIVER

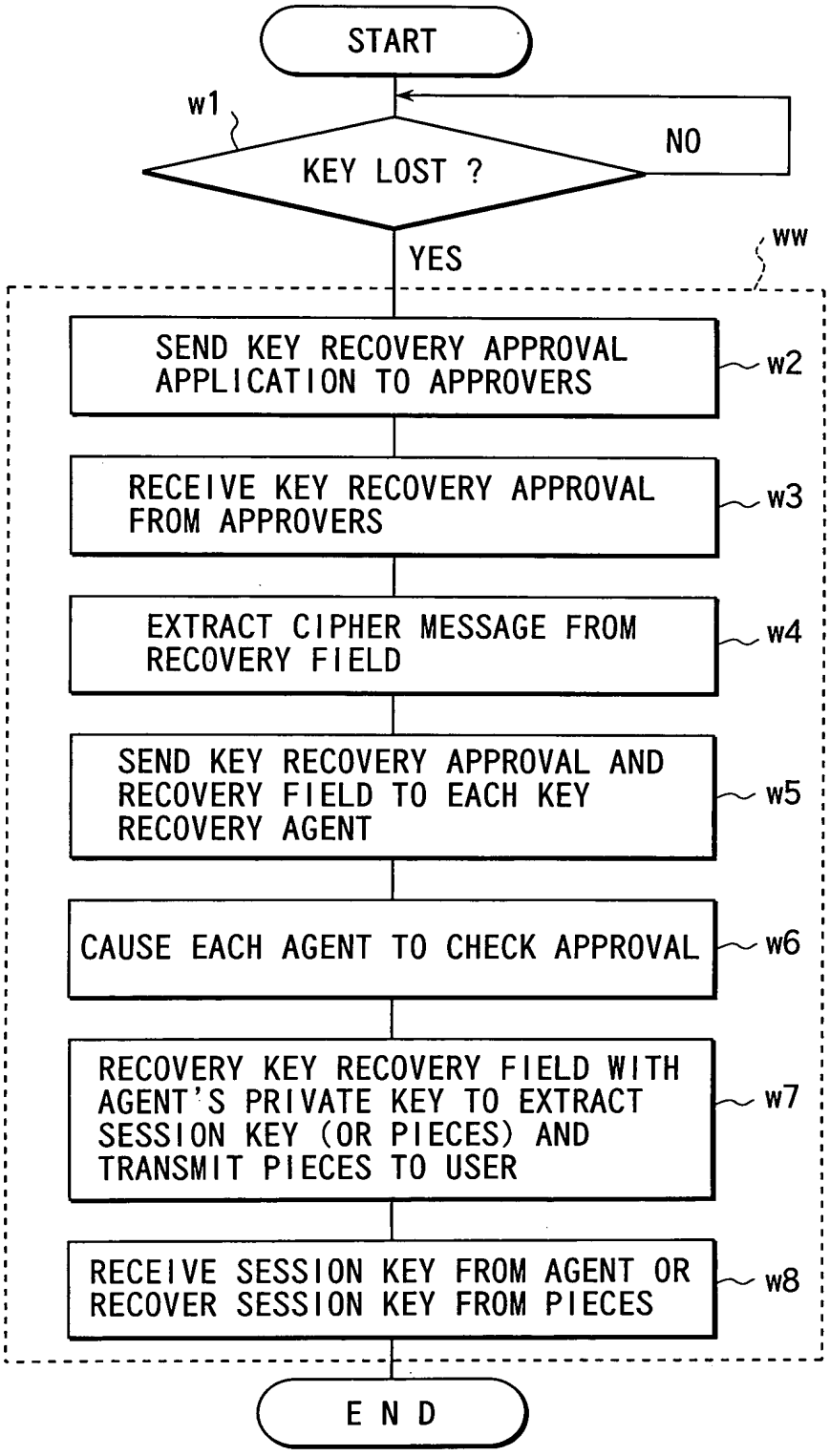

FIG.9

PROCEDURE FOR RECOVERING KEY BY THIRD PARTY

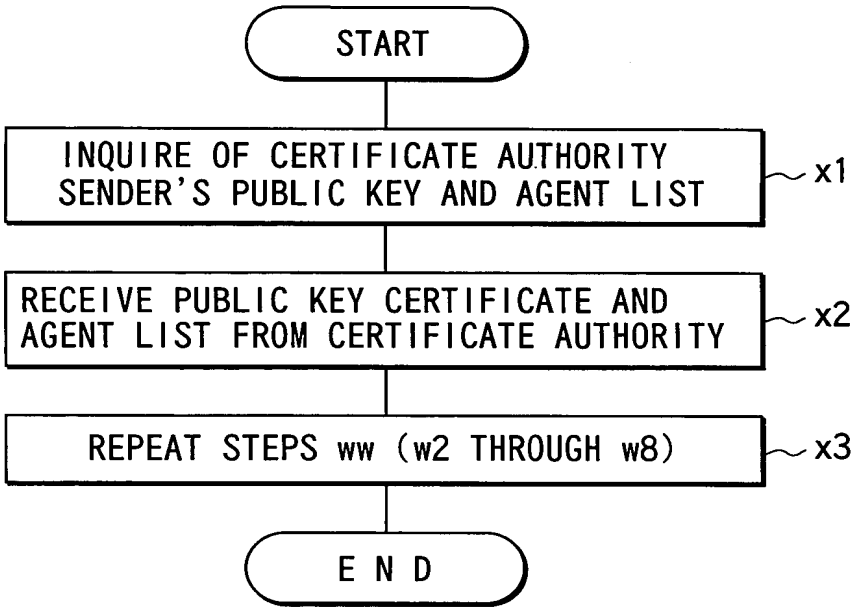

FIG.12

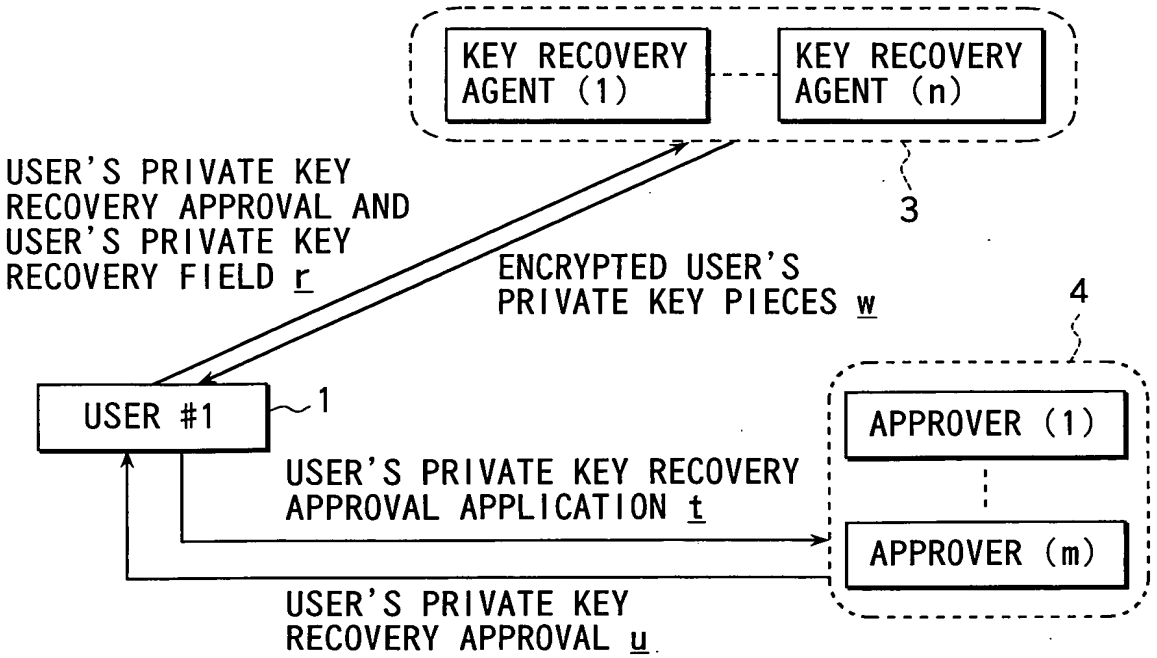

FIG.13